Senator Feinstein Calls for a Judiciary Committee Hearing on Legislation Requiring Notification when Personal Data is Compromised

February 16, 2005

Washington, DC – U.S. Senator Dianne Feinstein (D-Calif.) today called for a Senate Judiciary Committee Hearing on legislation that she sponsored which would require businesses or government agencies to notify individuals if a database has been broken into and personal data has been compromised, including Social Security numbers, driver's licenses and credit cards. This follows two recent incidents – involving databases at **Science Applications International Corporation** and **ChoicePoint** -- which underscore the need for federal legislation.

Following is a statement by Senator Feinstein:

"I strongly believe individuals have a right to be notified when their most sensitive information is compromised - because it is truly their information. And they have the right to decide what actions they want to take once a breach has been discovered. Unfortunately, data breaches are becoming all too common and current federal law does not require notification to consumers when these breaches occur. That's why I think we need to have a hearing in the Judiciary Committee and pass this bill through the Senate as soon as possible.

Consider the following incidents, which have compromised the records thousands of Americans:

- **Stockholders at Science Applications International Corporation (SAIC) learned that they were the victims of identity theft after a break-in resulted in the theft of several computers which contained personal information – names, Social Security numbers, addresses, telephone numbers and stockholder records, including shares bought, sold and held.**

- **ChoicePoint, a company that collects consumer data warned thousands of Californians that hackers penetrated the company's computer network and may have stolen credit reports, Social Security numbers, and other sensitive personal information.**

This legislation would take a step toward helping identity theft victims restore their identities by requiring government or private entities to promptly notify individuals if a data breach has compromised their Social Security number, driver's license number, credit card number, debit card number or financial account numbers. This would then allow them to take steps against fraud such as reviewing their credit reports, putting fraud alerts on their bank accounts, and carefully reviewing bank statements for suspicious activity."

A summary of Senator Feinstein’s bill follows:

The *"Notification of Risk to Personal Data Act"* would set a much-needed national standard for notification of consumers when a database breach occurs. Specifically, the legislation would:

- Require a business or government entity to notify an individual when there is a reasonable basis to conclude that a hacker or other criminal has obtained unencrypted personal data maintained by the entity;
- Define as personal data an individual's Social Security number, driver's license number, state identification number, bank account number, or credit card number;
- Subject entities that fail to comply with fines by the Federal Trade Commission of $5,000 per violation or up to $25,000 per day while the violation persists (State Attorneys General can also file suit to enforce the statute); and
- Allow California's new law to remain in effect, but preempt conflicting state laws, so as not to put companies in a situation that forces them to comply with database notification laws of 50 different states.

The legislation's notification scheme minimizes the burdens on companies or agencies that must report a database breach, and in general, notice would have to be provided to each person whose data was compromised in writing or through e-mail. But there are important exceptions:

- Companies that have developed their own reasonable notification policies are given a safe harbor under the bill and are exempted from its notification requirements;
- Encrypted data is exempted; and
- Where it is too expensive or impractical (e.g, contact address information is incomplete) to notify every individual who is harmed, the bill allows entities to send out an alternative form of notice called "substitute notice." Substitute notice includes posting notice on a website or notifying major media.

Substitute notice would be triggered if any of the following factors exist:

(i) the agency or person demonstrates that the cost of providing direct notice would exceed $250,000;
(ii) the affected class of subject persons to be notified exceeds 500,000; or
(iii) the agency or person does not have sufficient contact information to notify people whose information is at risk.

###